UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/560,579	04/23/2007	Scott MacDonald Ward	522331.0324476 (EPX0021-U	6641

36183 7590 03/09/2010

PAUL, HASTINGS, JANOFSKY & WALKER LLP
875 15th Street, NW
Washington, DC 20005

EXAMINER	
HENNING, MATTHEW T	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
03/09/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/560,579	WARD ET AL.	
	Examiner	Art Unit	
	MATTHEW T. HENNING	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 November 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

This action is in response to the communication filed on 11/30/2009.

DETAILED ACTION

Applicant's arguments filed 11/30/2009 have been fully considered but they are not persuasive.

Regarding the applicants' argument that Ginter did not teach that the authentication data was inaccessible to the user, the examiner does not find the argument persuasive. First, Ginter disclosed that the access keys were stored within the protected memory of the SPU. Second, Ginter teaches neither that the user has access to the access keys nor that the user has access to the protected memory of the SPU. Therefore, the examiner does not find the argument persuasive.

Regarding the applicants' argument that Ginter requires specific hardware not claimed, the examiner does not find the argument persuasive. The claims do not use the phraseology "consisting", but rather uses the phraseology "comprising". Therefore, the claims are not limited to only what has been recited within the claim language, but rather are limited to anything including what has been recited within the claim language. Therefore, the examiner does not find the argument persuasive.

Regarding the applicants' request for non-final rejection due to the applicants' belief that the rejection was not explained thoroughly enough, the examiner does not find the argument persuasive. The search report provides sufficient details as to how Ginter meets the claim language. Therefore, the examiner has maintained the rejection and has made the rejection final.

Regarding the applicants' argument that Cocotis does not teach wherein the authentication data is inaccessible to the user, the examiner does not find the argument

persuasive. Paragraph 0043 clearly states that in the case where the client is capable of communicating with the server, "then it is only necessary that the client 16 be able to access a public key corresponding to the private key used by the server 18." As such, in this case, the user does not have access to the public key. Therefore, the examiner does not find the argument persuasive.

Regarding the applicants' argument that a public key cannot be "authentication data" because it is predetermined, the examiner does not find the argument persuasive. Both public and private keys are used for authentication purposes. Therefore, they fall within the scope of "authentication data". As such, the examiner does not find the argument persuasive.

Regarding the applicants argument that Cocotis did not disclose "authentication software" in the user's electronic device, the examiner does not find the argument persuasive. Paragraphs 0043 and 0061 clearly show that a software application is present in the client 16, and that the software application contains the public key and is used to validate the server digital signatures. Therefore, Cocotis meets this limitation of the claim, and as such the examiner does not find the argument persuasive.

Regarding the applicants' argument that XTEC does not disclose that its cryptoprocessing key is inaccessible to the user, the examiner does not find the argument persuasive. First, XTEC does not teach the user ever having access to the cryptoprocessing key. Second, XTEC specifically states on Page 13 Lines 9-19 that the user cannot access the database because the key used to encrypt the database is not present in the system. Finally, it is the database that reads upon the authentication data in the claim language. As such, the examiner does not find the argument persuasive.

Regarding the applicants' argument that "using data supplied by a hard disk manufacturer to generate cryptoprocessing keys is clearly contrary to the present invention, the examiner does not find the argument persuasive. The examiner suggests that the claim language is broad enough to read upon the disclosure of XTEC, and therefore XTEC is relevant as prior art. As such, the examiner does not find the argument persuasive.

Regarding the applicants' argument that Cooper fails to teach that the authentication data is inaccessible to the user, the examiner does not find the argument persuasive. The examiner has not relied upon Cooper alone in teaching this limitation, but rather has relied upon the teachings of Cooper in combination with what was well known in the art at the time of invention (i.e. to make private keys inaccessible to users). Therefore, the examiner does not find the argument persuasive.

Regarding the applicants' argument that Cooper did not disclose authentication software that generates a digital signature, the examiner does not find the argument persuasive. The examiner has not relied upon Cooper alone in teaching this limitation, but rather has relied upon the teachings of Cooper in combination with the teachings of Mott. Therefore, the examiner does not find the argument persuasive.

Regarding the applicants' argument that Cooper did not disclose providing a digital signature to a second transaction party, the examiner does not find the argument persuasive. Col. 25 Line 40 – Col. 26 Line 24 clearly discloses where the user device generates a signature of the transaction ID, sends this signature to the customer site which verifies the signature, and embeds the signature into the content. Therefore, the examiner does not find the argument persuasive.

Regarding the applicants' argument that the combination of Cooper and Mott would result in a method in which a player retrieves an ID number from a digital information file, and verifying that the player ID matches the retrieved ID, the examiner does not find the argument persuasive. Mott clearly teaches that the signature of a content file should be verified prior to allowing playback of the content file. The combination would result in the player verifying the signature of the content file prior to allowing playback of the file. As the applicants have admitted, there would be no reason for incorporating the portion of Mott related to the ID numbers into Cooper. Therefore, the examiner does not find the argument persuasive.

Regarding the applicants' argument that there is no reason to combine Cooper with Mott, the examiner does not find the argument persuasive. The motivation to combine, as discussed in the rejection below, is that the ordinary person skilled in the art would have been motivated to ensure that the content had not been illicitly altered, and to ensure that the player would not play illicitly altered or copied content. Therefore, the examiner does not find the argument persuasive.

Regarding the applicants' argument that Cooper and Mott did not teach providing authentication data in a memory of an electronic device, the examiner does not find the argument persuasive. Cooper Col. 25 Line 40 – Col. 26 Line 24 clearly teaches that the private key is used by the player device to sign the transactional ID. Therefore the private key must have been present in a memory of the player device. Therefore, the examiner does not find the argument persuasive.

Regarding the applicants' argument that Cooper and Mott did not teach digital data having a digital signature embedded therein, the examiner points the applicants to Col. 25 Line

40 – Col. 26 Line 24 which clearly shows that the signed transactional ID may be transparently added to the digital content using watermarking technology. Therefore the examiner does not find the argument persuasive.

Regarding the applicants' argument regarding the means-plus-function language of claim 30, the examiner points out that the relied upon structures of Cooper and Mott are the equivalent of those disclosed in the present application, and the applicants have not presented any showing to the contrary. Therefore, the examiner does not find the argument persuasive.

Regarding the applicants' argument that Cooper/Mott/Challener do not teach storing or running authentication data or software that is inaccessible to the operating system of the device, the examiner does not find the argument persuasive. As discussed in the rejection of the claim below, the teachings of Challener in combination with the teachings of Cooper and Mott render these limitations obvious. That is, Challener teaches that the BIOS is used to verify signatures, thereby rendering obvious that the private key would be accessible only to the BIOS chip, and therefore not by the general operating system of the computer. As such, the examiner does not find the argument persuasive.

Regarding the applicants' argument that Cooper/Mott/Unicate do not teach an authentication table generated from a bit string which is generated from fixed and variable data and a bit string, the examiner does not find the argument persuasive. The teachings of Unicate meet the limitations claimed. For example, a first line of the image can read upon the fixed data, a second line of the image can read upon the string data, and the coordinates of the blanks in the image can read on the variable data. Therefore, the examiner does not find the argument persuasive.

All objections and rejections not set forth below have been withdrawn.

Claims 1-31 have been examined.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-5, 8-12, 14, and 29-30 are rejected under 35 U.S.C. 102(b) as being anticipated by Ginter et al. (US Patent Application Publication Number 2002/112171) for the reasons provided in the search report for PCT/NL2004/000422.

Claims 1-5, 8-12, 14, and 29-30 are rejected under 35 U.S.C. 102(b) as being anticipated by Cocotis et al. (US Patent Application Publication Number 2002/112162) for the reasons provided in the search report for PCT/NL2004/000422.

Claims 1, 2, 5-7, 10-11, 28, 29, and 31 are rejected under 35 U.S.C. 102(b) as being anticipated by XTEC (WO 01/84319).

Regarding claim 1, XTEC disclosed a method for performing an electronic transaction between a first transaction party and a second transaction party using an electronic device operated by the first transaction party, the method comprising: providing authentication data in a memory of said electronic device which authentication data are inaccessible to a user of said electronic device; providing authentication software in said electronic device, the authentication data being accessible to said authentication software; activating the authentication software to generate a digital signature from the authentication data; providing the digital signature to the second transaction party (XTEC Page 2 Line 19 - Page 4 Line 4, Page 5 Line 3 - Page 8 Line 19).

Regarding claim 28, XTEC disclosed a method for encrypting digital data on an electronic device using an encryption key, the method comprising: gathering session specific data; hashing said session specific data to obtain reference numbers referring to positions in an authentication table stored in said electronic device; generating said encryption key from the characters stored in the authentication table at said positions; and encrypting said digital data using said encryption key (XTEC Page 2 Line 19 - Page 4 Line 4, Page 5 Line 3 - Page 8 Line 19).

Regarding claims 2 and 29, XTEC disclosed a system for performing an electronic transaction between a first transaction party and a second transaction using an electronic device operated by the first transaction party, the system comprising: means for providing authentication data in a memory of said electronic device which authentication data are inaccessible to a user of the electronic device; means for providing authentication software in

said electronic device, the authentication data being accessible to said authentication software; means for activating the authentication software to generate a digital signature from the authentication data; means for providing the digital signature to the second transaction party; and means for providing digital data from the second transaction party to the first transaction party (XTEC Page 2 Line 19 - Page 4 Line 4, Page 5 Line 3 - Page 8 Line 19).

Regarding claim 31, XTEC disclosed a system for encrypting digital data using an encryption key, the system comprising: means for providing authentication data in a memory of said electronic device which authentication data are inaccessible to a user of the electronic device; means for providing authentication software in said electronic device, the authentication data being accessible to said authentication software; means for activating the authentication software to generate a digital signature from the authentication data; means for gathering session specific data; means for hashing said session specific data to obtain reference numbers referring to positions in an authentication table stored in said electronic device; means for generating said encryption key from the characters stored in the authorization table at said positions; and means for encrypting said digital data using said encryption key (XTEC Page 2 Line 19 - Page 4 Line 4, Page 5 Line 3 - Page 8 Line 19).

Regarding claims 5-7, XTEC disclosed wherein the authentication data are provided by the second transaction party, which stores the authentication data together with data identifying the first transaction party, (XTEC Page 2 Line 19 - Page 4 Line 4, Page 5 Line 3 - Page 8 Line 19), wherein the second transaction party uses the stored authentication data to obtain transaction specific authentication data according to a specific algorithm (XTEC Page 2 Line 19

- Page 4 Line 4, Page 5 Line 3 - Page 8 Line 19), wherein the second transaction party verifies the digital signature provided by the first transaction party using the authentication data stored at the second transaction party (XTEC Page 2 Line 19 - Page 4 Line 4, Page 5 Line 3 - Page 8 Line 19).

Regarding claims 10 and 11, XTEC disclosed wherein the authentication data are encrypted by the second transaction party using an encryption key before the authentication data are provided to the first transaction party, and wherein the authentication software retrieves a decryption key associated with the encryption key and decrypts the authentication data at its first use (XTEC Page 2 Line 19 - Page 4 Line 4, Page 5 Line 3 - Page 8 Line 19).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 6, 7, 13, and 15-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ginter et al. (US Patent Application Publication Number 2002/112171) for the reasons provided in the search report for PCT/NL2004/000422.

Claims 6, 7, 13, and 15-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cocotis et al. (US Patent Application Publication Number 2002/112162) for the reasons provided in the search report for PCT/NL2004/000422.

Claims 1-11, 14-18, and 29-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cooper et al. (US Patent Number 7,426,750) hereinafter referred to as Cooper, and further in view of Mott et al. (US Patent Number 6,170,060) hereinafter referred to as Mott.

Regarding claims 1 and 29, Cooper disclosed a system and method for performing an electronic transaction between a first transaction party and a second transaction party using an electronic device operated by the first transaction party, the method comprising: providing authentication data in a memory of said electronic device (Cooper Col. 9 Line 56- Col. 10 Line 14); generate a digital signature from the authentication data (Cooper Col. 29 Lines 17-26); providing the digital signature to the second transaction party (Cooper Col. 22 Line 35 – Col. 28 Line 6). Cooper failed to specifically disclose that authentication data are inaccessible to a user of said electronic device. However, it was well known in the art at the time of invention to secure authentication data, such as private encryption keys, from user access, and therefore, the ordinary person skilled in the art would have found it obvious to have done so. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the authentication data from being altered or exposed.

Cooper further failed to disclose providing authentication software in said electronic device, the authentication data being accessible to said authentication software; or activating the authentication software to generate the digital signature.

Mott teaches that in a content player, the signature in the content should be verified by the player prior to allowing the content to be played back (Col 19 Lines 18-37).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Mott in the system of Cooper by providing

authentication software for generating the signature and for verifying that the signature in the watermark matches the signature generated in the authentication software prior to permitting playback of the content. This would have been obvious because the ordinary person skilled in the art would have been motivated to ensure that the content had not been illicitly altered, and to ensure that the player would not play illicitly altered or copied content.

Regarding claims 9 and 30, Cooper and Mott taught a system and method for performing a verification of legitimate use of digital data on an electronic device, the method comprising: providing authentication data in a memory of said electronic device which authentication data are inaccessible to a user of the electronic device (Cooper Col. 9 Line 56- Col. 10 Line 14 and the rejection of claim 1 above); providing authentication software in said electronic device, the authentication data being accessible to said authentication software (Mott Col. 19 Lines 18-37 and the rejection of claim 1 above); activating the authentication software to generate a digital signature from the authentication data (Mott Col. 19 Lines 18-37 and the rejection of claim 1 above); providing the digital signature to the authentication software by an application accessing digital data having a digital signature embedded therein (Mott Col. 19 Lines 18-37 and the rejection of claim 1 above); and comparing the generated digital signature with the embedded digital signature (Mott Col. 19 Lines 18-37 and the rejection of claim 1 above).

Regarding claims 2-3 Cooper and Mott taught that the second transaction party provides digital data to the first transaction party, and that the second transaction party embeds the digital signature in the digital data provided to the first transaction party (Cooper Col. 22 Line 35 – Col. 28 Line 6 and Col. 29 Lines 17-26).

Regarding claim 4, Cooper and Mott taught that the second transaction party stores the digital signature together with data identifying the first transaction party (Cooper Col. 29 Lines 17-26).

Regarding claims 5-7, Cooper and Mott taught wherein the authentication data are provided by the second transaction party, which stores the authentication data together with data identifying the first transaction party, wherein the second transaction party uses the stored authentication data to obtain transaction specific authentication data according to a specific algorithm, wherein the second transaction party verifies the digital signature provided by the first transaction party using the authentication data stored at the second transaction party (Cooper Col. 16 Line 49 – Col. 21 Line 10).

Regarding claim 8, Cooper and Mott taught that the first transaction party further provides a signed digital signature to the second transaction party, the signed digital signature being generated by the authentication software by signing the digital signature using a private key, which private key is unique for said authentication software and is known to a third party (See the rejection of claim 1 above).

Regarding claims 10-11, Cooper and Mott taught that the authentication data are encrypted by the second transaction party using an encryption key before the authentication data are provided to the first transaction party, and wherein the authentication software retrieves a decryption key associated with the encryption key and decrypts the authentication data at a first use of the authentication data (Cooper Col. 29 Lines 17-26 and the rejection of claim 1 above).

Regarding claims 14-18, while Cooper and Mott did not specifically teach that the authentication data are encrypted when the authentication data are stored in said memory, and

wherein a decryption key for decrypting the authentication data is inaccessible to said user and to any user-operated software, thereby rendering the authentication data inaccessible to said user, wherein the authentication data are encrypted using at least two encryption layers, wherein at least one encryption layer may be decrypted using a decryption key associated with at least one serial number of hardware a component of said electronic device, wherein at least one encryption layer may be decrypted by the authentication software, and wherein the authentication data are decrypted in a secure processing, environment inaccessible to said user and to any user-operated software, these were well known features of secure storage in the art at the time of invention, and as such, would have been obvious to the ordinary person skilled in the art at the time of invention.

Claims 12-13 and 26-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cooper and Mott as applied to claim 1 above, and further in view of Challener et al. (US Patent Application Publication 20030208338) hereinafter referred to as Challener.

While Cooper and Mott taught that the authentication data was inaccessible to the user, Cooper and Mott failed to specifically teach that the memory was inaccessible to an operating system of the electronic device, that the authentication data are provided in a BIOS of the electronic device, or that the authentication software is inaccessible to an operating system and is run in a secure processing environment.

Challener teaches that in many computer platforms, trusted information such as private keys, digital certificates, random number generators, protected storage and the Root-of-Trust Measurement, reside on two hardware chips within the platform, the Trusted Platform Module

(TPM) and the POST/BIOS Module (Challener Paragraph 0018). Challener further teaches that the BIOS is used to verify signatures (Challener Paragraph 0028).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Challener in the signature verification content player system of Cooper and Mott by storing the authentication data, such as the private and public keys, in the BIOS, and having the BIOS routines perform the authentication. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide a specific means to the generic teachings for storing the authentication data and for implementing the verification processing.

Claims 19-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cooper and Mott as applied to claim 1 above, and further in view of Unicate (WO 00/67143).

While Cooper and Mott disclosed authentication of a signature, Cooper and Mott failed to specifically disclose the authentication data comprise an authentication table, wherein the authentication table is generated from a bit string which is generated from fixed data and variable data, wherein the fixed data are at least part of a serial number of a hardware device, wherein the fixed data are at least part of a device specific software identification code of the authentication software, wherein the variable data comprise a random table, wherein the random table is calculated from a random two-dimensional or three-dimensional pattern, or wherein the authentication table is generated from fixed data, variable data and a bit string, which bit string is specific to a trusted third party that provides the authentication data.

Unicate teaches an authentication system wherein the authentication data comprise an authentication table, wherein the authentication table is generated from a bit string which is

generated from fixed data and variable data, wherein the fixed data are at least part of a serial number of a hardware device, wherein the fixed data are at least part of a device specific software identification code of the authentication software, wherein the variable data comprise a random table, wherein the random table is calculated from a random two-dimensional or three-dimensional pattern, or wherein the authentication table is generated from fixed data, variable data and a bit string, which bit string is specific to a trusted third party that provides the authentication data (Page 13 Line 34 – Page 15 Line 2).

It would have been obvious to the ordinary person skilled in the art at the time of invention to have employed the teachings of Unicate in the content player system of Cooper and Mott by employing the authentication table for generating the signatures to be embedded in the content. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide a secure transaction without the need for cryptography.

Conclusion

Claims 1-31 have been rejected.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MATTHEW T. HENNING whose telephone number is (571)272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571)272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Matthew T Henning/
Primary Examiner, Art Unit 2431